UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/764,918	01/26/2004	Michael F. Angelo	200314543-1	2632

22879 7590 11/02/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
DOAN, DUC T	

ART UNIT	PAPER NUMBER
2185	

NOTIFICATION DATE	DELIVERY MODE
11/02/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MICHAEL F. ANGELO,
LARRY N. MCMAHAN, and RICHARD D. POWERS

Appeal 2009-005587
Application 10/764,918
Technology Center 2100

Before: HOWARD B. BLANKENSHIP, ST. JOHN COURTENAY III, and DEBRA K. STEPHENS, *Administrative Patent Judges*.

STEPHENS, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

Appellants appeal under 35 U.S.C. § 134(a) (2002) from the non-final rejection mailed September 21, 2007 of claims 1-26, and 31-34. Claims 27 and 28 have been allowed. Claims 29 and 30 have been canceled. (Br. 2). We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We AFFIRM.

Introduction

According to Appellants, the invention relate to a security module and a method and apparatus for operating multiple security modules (Spec., Title, 1, 2 and Abstract).

STATEMENT OF CASE

Exemplary Claim(s)

Claim 1 is an exemplary claim and is reproduced below:

1. A method of operating a first security module in a computer, the method comprising the acts of:

detecting a second security module in the computer, wherein the second security module is configured to perform the same functions as the first security module;

determining whether a key associated with the second security module is stored at the first security module; and

obtaining the key associated with the second security module if the key associated with the second security module is not stored at the first security module.

Prior Art

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Challener	US 2003/0174842 A1	Sep. 18, 2003
Dickinson	US 7,187,771 B1	Mar. 6, 2007

Appellants' background (Spec. "Background of the Related Art" [0001]-[0004]), hereinafter AB.

REJECTIONS

Claims 8-20 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter (Ans. 3).

Claims 1-26, 31, and 32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over AB, and Challener (Ans. 4).

Claims 33 and 34 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over AB, Challener, and Dickinson (Ans. 7).

GROUPING OF CLAIMS

(1) Appellants argue the 35 U.S.C. § 101 rejection of claims 8-20 as a group on the basis of independent claims 8 and 14 (App. Br. 6-8). We accept independent claims 8 and 14 as the representative claims. We will, therefore, treat dependent claims 9-13 and dependent claims 15-20 as standing or falling with representative claims 8 and 14 respectively.

(2) Appellants argue claims 1-4, 6-11, 13-17, 19, 20, 22-24, and 26-32 as a group on the basis of independent claims 1, 8, 14, 21, and 31 (*id.* at 8-13). We select independent claim 1 as the representative claim. We will,

therefore, treat claims 2-4, 6-11, 13-17, 19, 20, 22-24, and 26-32 as standing or falling with representative claim 1.

(3) Appellants argue claims 5, 12, 18, and 25 separately as a group (*id.* at 14). We select dependent claim 5 as the representative claim. Thus, claims 12, 18, and 25 stand or fall with representative claim 5.

(4) Appellants argue claims 33 and 34 as a group (*id.* at 15-17). We select independent claim 33 as the representative claim. We will, therefore, treat claim 34 as standing or falling with representative claim 33.

We accept Appellants' grouping of the claims. *See* 37 C.F.R. § 41.37(c)(1)(vii).

ISSUE 1

35 U.S.C. § 101 claims 8-20

Appellants argue their invention is not directed to non-statutory subject matter because they are directed to apparatuses and recite discreet physical structures. (App. Br. 7 and Reply Br. 2). More specifically Appellants state since their software is in a tangible medium, it is patentable subject matter (App. Br. 7 and 8 and Reply Br. 2 and 3). Additionally, according to Appellants, the security module is described in the specification as including physical structure (App. Br. 7).

In response, the Examiner maintains that the

> specification's paragraph 21 clearly states that the detection and the key could be merely some code/software ("the detection 82 and the key obtaining device 84 may be implement in hardware, software, or any combination thereof '). And because these only two structures are claimed in the body, and both of them (the detector and the device) can be implemented as software

> only as stated in the specification. Thus the claim does not have any physical structure being claimed and fails to fall within the statutory of invention;

(Ans. 9, emphasis original).

Issue 1: Has the Examiner erred in finding that claims 8-20 are directed to non-statutory subject matter?

FINDINGS OF FACT (FF)

Appellants' Invention

(1) The security module 80 described may include a detector 82 and a key obtaining device 84 as well as various other components not shown. "The detector 82 and the key obtaining device 84 may be implemented in hardware, software, or any combination thereof, which may be individual components or combined into a single device." (Spec. 7, [0021]).

ANALYSIS

The subject matter of claims permitted within 35 U.S.C. § 101 must be a machine, a manufacture, a process, or a composition of matter. Moreover, our reviewing court has stated that "[t]he four categories [of § 101] together describe the exclusive reach of patentable subject matter. If the claim covers material not found in any of the four statutory categories, that claim falls outside the plainly expressed scope of § 101 even if the subject matter is otherwise new and useful." *In re Nuijten*, 500 F.3d 1346,

1354 (Fed. Cir. 2007); *accord In re Ferguson*, 558 F.3d 1359 (Fed. Cir. 2009). This latter case held that claims directed to a "paradigm" are non-statutory under 35 U.S.C. § 101 as representing an abstract idea.

We agree with the Examiner that the scope of claim 8 could encompass non-statutory subject matter. Claim 8 recites a first security module that comprises only two recited elements: a detector and a device, as shown in Figure 2. Appellants have stated in their Specification that both of these devices can be software only (FF 1). Accordingly, the security module itself may be software only.

Appellants' argument that the security modules are described as including physical structure is unpersuasive. Appellants use the terms "may include" in describing the elements of the computer system and thus, the security module is not defined as having physical components. Moreover, claim 8 does not recite any physical components but only two non-physical components: a detector and a device.

Claim 14 also recites a first security module. Although Appellants again argue their Specification provides physical structure, we find these arguments unpersuasive. Appellants rely on discussion of a trusted platform module (TPM); however, a TPM is given as an example of a security module (FF 2). Additionally, as previously stated, Appellants' language in their Specification uses exemplary words such as "may include;" therefore, a processor or memory given as an example does not limit the claim to such physical structures.

Thus, claims 8 and 14 may be broadly but reasonably construed as encompassing software. Laws of nature, abstract ideas, and natural phenomena are excluded from patent protection. *Diamond v. Diehr*, 450

U.S. 175, 185 (1981). A claim that recites no more than software, logic or a data structure (i.e., an abstraction) does not fall within any statutory category. *In re Warmerdam*, 33 F.3d 1354, 1361 (Fed. Cir. 1994). Accordingly, we find Appellants have not shown the Examiner erred in concluding claims 8 and 14, and their dependent claims 9-13 and 15-20 recite non-statutory subject matter.

ISSUE 2

35 U.S.C. § 103(a): claims 1-4, 6-11, 13-17, 19, 20, 22-24, and 26-32.

Appellants assert their invention is not obvious over AB and Challener because neither AB, Challener nor a combination thereof discloses multiple security modules in a single computer nor teaches "the second security module is configured to perform the same functions as the first security module," as commensurately recited in claims 1, 8, 14, 21, and 31 (App. Br. 11-12). Appellants argue Challener does not teach two security modules configured to perform the same function (App. Br. 13). Further, Appellants state that AB cited by the Examiner does not qualify as prior art nor an admission of prior art by Appellants because Appellants have specifically stated that the statements are not an admission of prior art and are presented merely to facilitate an understanding of their invention. (App. Br. 12). Appellants contend in their Reply Brief that the Examiner's introduction of the Dickenson reference to bolster the rejection is not proper since this is a new reference which has not been applied to the claims at issue previously (Reply Br. 4).

The Examiner finds with respect to Appellants' objection of AB as being non-prior art:

> Examiner has carefully reviewed the background of the relate[d] art and believe this section clearly teaches the facts that have been known in the field of computer system including multiple security modules in a single computer system (paragraphs 3 and 4) and multiple security modules are doing the same functions. For example, AB teaches commonly known functions that every security module must [perform] such as encrypting and decrypting data with proper keys, paragraph 3 lines 6-7. And of course, security modules in a computer system must carries [sic] out all same commonly known functions such as encrypting and decrypting data (paragraph 2 lines 5-7).

(Ans. 10). The Examiner also finds that Challener teaches two security modules performing the same function – functions which are present in any security module (i.e., hashing, generating and obtaining keys, and asymmetrical key encryption/decryption, for example).

Issue 2: Have Appellants shown the Examiner erred in (i) taking Official Notice or providing the Dickenson reference as support; and (ii) finding that the combination of references teaches a computer with two security modules, "wherein the second security module is configured to perform the same functions as the first security module?"

FURTHER FINDINGS OF FACT (FF)

Challener

(2) Challener teaches a method and system for storing a private key created on a client computer by a user, on a server (Abstract).

(3) A computer system includes a Trusted Computer Platform Alliance (TCPA) enabled client computer 12 connected via a network to at least one TCPA-enabled server 16 (pg. 2, [0021]). Both the server 16 and the client computer 12 include a Trusted Platform Modules (TPM) 40 and 22, respectively (pg. 2, [0022]). The TCPA subsystem, "typically using a hardware chip called a Trusted Platform Module (TPM), uses cryptographic algorithms based on RSA…to generate public/private key pairs…A TCPA-enabled computer contain a TPM…and is able to perform cryptology functions as defined by the TCPA standards" (pg. 1, [0006]).

Dickenson

(4) A secure server, or trust engine, stores cryptographic keys and user authentication data on a server. Users can access the cryptographic functionality through the network and trust engine. (Abstract).

(5) One aspect of the invention includes a secure authentication system comprising multiple authentication engines. Each of the authentication engines receives enrollment authentication data and current authentication data which are compared to each other to produce an authentication result. The secure authentication system also includes a redundancy system which receives the authentication result from two or more authentication engines to determine if a user has been uniquely identified. (Col. 5, ll. 55-67).

(6) The trust engines may or may not be geographically separated (Col. 32, ll. 4-6). Which trust engine(s) to use may be based on the

availability, operability, speed of connections, load, performance, geographic proximity, or a combination thereof. (Col. 32, ll. 43-56).

ANALYSIS

Issue i

The Examiner relies on Official Notice to support his contention that the computer environment wherein a computer has two security modules is known in the art (Ans. 11). The Examiner's further relies on Appellant's AB and Dickenson to support the finding that this concept was indeed well known in the art at the time of the invention. Appellants' belief that the Examiner has introduced new grounds of rejection by providing Dickenson as support for the Official Notice is a petitionable matter and therefore, not a matter before the Board.

> IV. REQUEST FOR DESIGNATION AS NEW GROUND OF REJECTION
> Appellant cannot request to reopen prosecution pursuant to 37 CFR 41.39(b) if the examiner's answer does not have a new ground of rejection under 37 CFR 41.39. If appellant believes that an examiner's answer contains a new ground of rejection not identified as such, appellant may file a petition under 37 CFR 1.181(a) within two months from the mailing of the examiner's answer requesting that a ground of rejection set forth in the answer be designated as a new ground of rejection. Any such petition must set forth a detailed explanation as to why the ground of rejection set forth in the answer constitutes a new ground of rejection. Any allegation that an examiner's answer contains a new ground of rejection not identified as such is waived if not timely raised (i.e., by filing the petition within two months of the answer) by way of a petition under 37 CFR 1.181(a).

MPEP §1207.03 (IV)

In the Reply Brief, Appellants fail to traverse the Examiner's finding that redundancy in computers, e.g., using multiple security modules in a computer, was well known in the art at the time of the invention. Instead, Appellants argue that the cited art may not be used to support this finding.

We therefore find Appellants have not shown the Examiner erred in finding that a computer having two security modules would have been well known in the art at the time of the invention. Moreover, we find that Dickenson discloses a computer having more than one security module in the computer (FF 5 and 6). Appellants' argument that Dickenson requires the trust engines be geographically separated is unsupported by Dickenson. Dickenson describes a trust engine system with multiple trust engines and then presents "one embodiment" where each of the trust engines are geographically separated (*See* col. 32, ll. 4-6). We also find that AB discloses a computer having more than one security module, which as discussed above, was a well known technique at the time the invention was made.

Issue ii

We determine the scope of the claims in patent applications not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction in light of the specification as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). The properly interpreted claim must then be compared with the prior art.

Challener teaches a computer system that includes two computers, each of which has a TPM (FF 5). The TPM is able to perform function

defined by the TCPA standards (*id*). Therefore, each TPM in Challener is configured to perform the same functions – those defined by the TCPA standards. Appellants' argument that the security modules perform different functions is irrelevant.

Thus, Appellants have not persuaded us that the Examiner erred in (i) taking Official Notice; and (ii) finding that the combination of references teaches a computer with two security modules, "wherein the second security module is configured to perform the same functions as the first security module. Accordingly, Appellants have failed to persuade us of error in the Examiner's conclusion that the invention as recited in claim 1, and commensurately recited in claims 8, 14, 21, and 31 is obvious under 35 USC §103. Claims 2-4, 6, 7, 9-11, 13, 15-17, 19, 20, 22-24, 26-30 and 32 were not separately argued but grouped with arguments set forth for claim 1. Accordingly, Appellants have not shown the Examiner erred in rejecting claims 1-4, 6-11, 13-17, 19, 20, 22-24, and 26-32.

ISSUE 3

35 U.S.C. § 103(a): claims 5, 12, 18, and 25

Appellants assert their invention is not obvious over AB and Challener because Challener does not teach the step of "sending of a 'public key along with validation information' from the first security module to a the second (or other) security module if the key associated with the second (or other) security module is not stored at the first security module" (App. Br. 14). Instead, according to Appellants, Challener teaches that migrating of a private key must be authorized through an authorization sent independent of any keys (*id.*).

The Examiner finds that Challener's teaches authorization data and a public key can be sent with the private key and thus, Challener teaches sending a pubic key and authorization information (Ans. 14).

Issue 3: Have Appellants shown the Examiner erred in finding that Challener teaches "sending of a public key along with validation information from the first security module to the second security module" as recited in claim 5 and commensurately recited in claims 12, 18, and 25?

FURTHER FINDINGS OF FACT (FF)

Challener

(7) A private key can be migrated to another computer. First a determination is made whether the user's private key is stored on the server. If not, and it is determined the client computer can migrate the user's private key to the server, the user's private key is then migrated. "The private key is wrapped with a public non-migratable key of the server to form a first 'blob,' and the first blob is then sent to the server." A determination is then made whether further migration to other client computers is permitted and if permitted, migration through formed blobs occurs. (pg. 3, [0028] - [0030] and Fig. 3).

(8) In a preferred embodiment, a client user must first authorize migrating the user's private key to the server and requesting the user's private key from the server to a specific client computer. "This authorization is preferably performed by transmitting authorization data

using keyed-has message authentication code (HMAC)…well known to those skilled in the art of cryptology." (pg. 3, [0031]).

ANALYSIS

We agree with the Examiner's findings that Challener teaches a private key and a public key being transmitted together (FF 7). We also agree with the Examiner's findings that Challener teaches authorization data being sent in response to migrating the user's private key to the server and requesting the user's private key from the server to a specific client computer (FF 8). Thus, we find Challener teaches the public key and the validation information are sent from the first security module to the second security module. Appellants have not provided any arguments or evidence to persuade us that the Examiner erred in finding Challener teaches or suggests "sending a public key along with validation information." Accordingly, Appellants have failed to persuade us of error in the Examiner's rejection of claims 5, 12, 18, and 25 for obviousness.

ISSUE 4

35 U.S.C. § 103(a): claims 33 and 34

Appellants assert their invention is not obvious over AB, Challener, and Dickenson, because the addition of Dickenson in this rejection does not overcome the deficiencies found in parent claims 1 and 8 of the previous § 103(a) rejection. Moreover, Appellants contend that that the applied prior art does not disclose the limitation of a first security module accessing data encrypted by a second or other security module if the second or other security module fails, as similarly recited in claims 33 and 34 (App. Br. 16-

17). Instead, according to Appellants, Dickenson only discloses the authentication engine has current data to compare to determine an authentication result (App. Br. 17 and Reply Br. 8).

The Examiner finds Dickenson teaches that one of the security modules can be used in a redundant manner, so that the overall system can operate if one of the security modules (trust engines) fails. (Ans. 15).

Issue 4*:* Has the Examiner erred in concluding that the combination of Challener, AB, and Dickenson teaches or suggest "a first security module accessing data encrypted by a second or other security module if the second or other security module fails?"

ANALYSIS

As discussed previously in Issues 2 and 3, the combination of Challener and Official Notice teaches two security modules in a computer performing the same function; therefore, Appellants' arguments regarding the lack of teaching of two security modules in a computer performing the same function have been addressed.

We find Dickenson teaches a system having a redundancy system which receives an authentication result from two of more authentication engines (FF 5). Dickenson also teaches that which trust engine(s) are used may be based on availability or operability as well as other criteria (FF 6). Additionally, we find the Examiner is relying on Dickenson as teaching redundant trusted engines which control several redundant copies of critical data (Ans. 7 and 8).

Appellants do not present any additional arguments or evidence that Dickenson does not teach the first module accessing data encrypted by the second security module if the second security module fails. As clarified in *KSR*, the skilled artisan is "a person of ordinary creativity, not an automaton." *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 421 (2007). Moreover, Appellants have presented no argument or evidence that using the redundancy system of Dickenson in the system of Challener and AB (or Official Notice) would have been "uniquely challenging or difficult for one of ordinary skill in the art" or "represented an unobvious step over the prior art." *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 418). Thus, we conclude one of ordinary skill in the art would have found it obvious to use the technique of Dickenson to provide redundant functionality in the security modules (trusted engines) in case of failure.

The Examiner relies on the combination of Challener, AB, and Dickenson as the basis for the obviousness rejection. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references ((*In re Keller*, 642 F. 2d 413, 426 (CCPA 1981); *In re Merck & Co., Inc.*, 800 F. 2d 1091, 1097 (Fed. Cir. 1986)). Appellants have presented no arguments or evidence that the combination of Challener and AB would not have taught or suggested accessing data encrypted by the second security module using the key associated with the second security module.

Therefore, Appellants have failed to persuade us that the Examiner erred in finding the combination of Challener, AB, and Dickenson teaches or at least suggests the first security module "accessing data encrypted by the

second security module if the second security module fails" as recited in claim 33. No additional arguments were presented for claim 34 which depends from claim 33. Accordingly, Appellants have not shown the Examiner erred in concluding claims 33 and 34 are obvious over Challener, AB, and Dickenson.

CONCLUSION

Appellants have not shown the Examiner erred in rejecting claims 8-20 under 35 U.S.C. § 101 as being directed to non-statutory subject matter.

Appellants have not shown that the Examiner erred in rejecting claims 1-26, 31 and 32 under 35 U.S.C. § 103(a) for obviousness over AB and Challener.

Appellants have not shown the Examiner erred in rejecting claims 33 and 34 under 35 U.S.C. § 103(a) for obviousness over AB, Challener, and Dickenson.

DECISION

The Examiner's rejection of claims 8-20 under 35 U.S.C. § 101 as being directed to non-statutory matter is affirmed.

The Examiner's rejection of claims 1-26, 31 and 32 under 35 U.S.C. § 103(a) as being obvious over AB and Challener is affirmed.

The Examiner's rejection of claims 33 and 34 under 35 U.S.C. § 103(a) as being obvious over AB, Challener, and Dickenson is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv) (2010).

AFFIRMED

Vsh

HEWLETT-PACKARD COMPANY
INTELLECTUAL PROPERTY ADMINISTRATION
3404 E. HARMONY ROAD
MAIL STOP 35
FORT COLLINS CO 80528